UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,566	01/25/2002	Dennis Michael Volpano	CRAN0006	4666

22862 7590 09/28/2005

GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 09/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/057,566	VOLPANO, DENNIS MICHAEL	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30 and 32-37* is/are rejected.

7)☒ Claim(s) *31* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(e).

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-3,5-7,9-11,15,17,19-23,33, and 34 are rejected under 35 U.S.C. 102(b) as being anticipated by Yuasa et al, U.S. Patent 6,085,238.

As per claim 1, Yuasa et al teaches of an apparatus for segregating traffic amongst a plurality of stations that are associated with an access point, comprising a LAN segment, and a personal virtual bridged local area network (personal VLAN) for partitioning said LAN segment logically into multiple virtual bridged local area networks (VLANs)(col. 9, lines 15-25 & 33-45; col. 10, lines 48-67).

As per claim 2, it is disclosed by Yuasa et al that the personal VLAN further comprising a VLAN bridge for forwarding unicast and group frames only to those ports that serve the VLAN to which the frames belong (col. 9, lines 3-15 and col. 38, lines 45-56).

As per claim 3, it is taught by Yuasa et al that the personal VLAN further comprising a protocol for VLAN discovery (col. 9, lines 3-15).

As per claim 5, Yuasa et al teaches of one or more logical ports in which a Personal VLAN bridge can maintain more than one logical port per physical port, and bridges between ports of any kind (col. 79, lines 4-20).

As per claim 6, Yuasa et al discloses of means for cryptographic VLAN separation in which in a Personal VLAN, a logical port serves at most one VLAN but, because there may be more than one logical port per physical port, more than one VLAN may exist on a physical port (col. 45, lines 13-17 and col. 79, lines 4-20).

As per claim 7, it is disclosed in the teachings of Yuasa et al that traffic within one VLAN is separated from another VLAN on a same physical port by cryptography (col. 45, lines 13-17).

As per claim 9, Yuasa et al recites of an extended protocol comprising the IEEE 802.1x-1998 (Virtual Bridged LANs) protocol (col. 25, line 53 through col. 26, line 3).

As per claim 10, it is taught by Yuasa et al of means for providing layer-2 VLAN support across routers (col. 5, line 63 through col. 6, line 9).

As per claim 11, Yuasa et al discloses of means for implementing a spanning tree algorithm when a personal VLAN permits an STA to create a VLAN where the STA itself is a bridge (col. 23, lines 13-32).

As per claim 15, Yuasa et al teaches of a method for segregating traffic amongst a plurality of stations that are associated with an access point, comprising the steps of providing a protocol for virtual local area network (VLAN) discovery, allowing a station to

create a new port that serves a new VLAN, or to join an existing VLAN maintaining more than one logical port per physical port, and providing cryptographic VLAN separation, wherein traffic within one VLAN is separated from another VLAN on a same physical port by cryptography (col. 9, lines 3-25 & 35-45; col. 10, lines 48-67; col. 45, lines 13-17; and col. 79, lines 4-20).

As per claim 17, Yuasa et al discloses of providing an encryption mechanism for keeping traffic private except to members of said VLAN (col. 45, lines 13-17).

As per claim 19, Yuasa et al teaches of a system for segregating traffic amongst a plurality of stations that are associated with an access point, an apparatus for virtual local area network (VLAN) discovery, comprising: a personal VLAN bridge for partitioning a LAN segment logically into multiple VLANs; and server and client VLAN discovery agents associated with said VLAN bridge for discovering other VLANs and/or allowing VLANs that said VLAN bridge serves to be discovered (col. 1, lines 20-32; col. 9, lines 3-25 & 33-45; and col. 10, lines 48-67).

As per claim 20, the teachings of Yuasa et al disclose of means for transmitting a discover frame (col. 9, lines 3-15).

As per claim 21, Yuasa et al discloses of means for transmitting a VLAN-OFFER frame to a source MAC address of said discover frame, wherein said offer frame lists at least some of the VLANs served by a bridge and information that can be used to select from among them (col. 9, lines 3-15 and col. 19, line 34 through col. 20, line 12).

As per claim 22, it is disclosed by Yuasa et al of means for receiving a request to serve a new VLAN (col. 9, lines 45-53).

As per claim 23, it is taught by Yuasa et al that the request contains a virtual LAN ID (VID) of a new VLAN (col. 9, lines 45-53).

As per claim 33, it is recited in the teachings of Yuasa et al of an apparatus for segregating traffic amongst stations (STAs) that are associated with a bridge, comprising a personal virtual bridged local area network (personal VLAN) that uses a VLAN to segregate traffic (col. 1, lines 20-32; col. 9, lines 3-25 & 33-45; and col. 10, lines 48-67).

As per claim 34, the teachings of Yuasa et al recites of means associated with said personal VLAN for partitioning a LAN segment logically into multiple VLANs, and a personal VLAN bridge associated with said personal VLAN for forwarding unicast and group frames only to those ports that serve a VLAN to which said frames belong (col. 1, lines 20-32; col. 9, lines 3-15; and col. 38, lines 45-56).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 4,8,12-14,16,18,24-30,32, and 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yuasa et al, U.S. Patent 6,085,238 in view of Gage et al, U.S. Patent 6,035,405.

As per claims 4,8,16, and 18, the teachings of Yuasa et al disclose of the use of encryption to keep traffic private except to members of the VLAN (col. 45, lines 13-17), but fails to disclose of means for allowing a station to join an existing VLAN via an authentication protocol wherein the authentication code uniquely identifies a VLAN to which traffic belongs. Gage et al teaches of means for allowing a station to join an existing VLAN via an authentication protocol wherein the authentication code uniquely identifies a VLAN to which traffic belongs (col. 2, lines 17-44). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply authentication of parties in order to determine if they are authorized to gain access. The teachings of Gage et al recites motivation for the use of authentication by disclosing that it can keep track of which members belong to a VLAN and to avoid unauthorized parties connecting to a VLAN (col. 2, lines 7-10 & 20-26). It is obvious that the teachings of Yuasa et al would have been improved by incorporating the teachings of Gage et al as a means of ensuring that authentic parties are authorized to access a VLAN.

As per claim 12, Yuasa et al discloses of a method for segregating traffic amongst a plurality of stations that are associated with an access point, comprising the steps of providing a distribution system comprising multiple virtual local area networks (VLANs), wherein every station that associates with said access point can create a new VLAN with itself and said distribution system as its members, and separating traffic between trusted and untrusted stations even though they associate with a same access point (col. 9, lines 15-25 & 33-45; col. 10, lines 48-67; and col. 45, lines 13-17). The

teachings of Yuasa et al fail to disclose of wherein a creator of a new VLAN can authenticate stations that wish to join said new VLAN. It is disclosed by Gage et al of a creator of a new VLAN can authenticate stations that wish to join said new VLAN (col. 2, lines 17-44). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply authentication of parties in order to determine if they are authorized to gain access. The teachings of Gage et al recites motivation for the use of authentication by disclosing that it can keep track of which members belong to a VLAN and to avoid unauthorized parties connecting to a VLAN (col. 2, lines 7-10 & 20-26). It is obvious that the teachings of Yuasa et al would have been improved by incorporating the teachings of Gage et al as a means of ensuring that authentic parties are authorized to access a VLAN.

As per claim 13, Yuasa et al recite of the step of discovering existing VLANs (col. 9, lines 3-15).

As per claim 14, Yuasa et al discloses of comprising the step of joining an existing VLAN (col. 9, lines 3-15).

As per claim 24, Yuasa et al teaches of 24. In a system for segregating traffic amongst a plurality of stations that are associated with an access point, a method for requesting service for a new virtual local area network (VLAN), comprising the steps of a bridge receiving a request frame with a source MAC address through a control channel of a physical port, wherein a holder of said MAC address is a requester, receiving said request frame initiating an authentication protocol with said requester through said control channel, creating a new logical port and associating said new

logical port with a physical port through which said request frame is received if there is no-conflict in using a virtual LAN ID (VID) requested, otherwise, said bridge negotiating a VID with said requester; and updating port state information for said logical port to include a security association, shared with said requester, that is in effect for all traffic through said port (col. 9, lines 15-25 & 33-45; col. 10, lines 48-67; col. 19, line 34 through col. 20, line 12; and col. 45, lines 13-17). The teachings of Yuasa et al fail to disclose of receiving said request frame initiating an authentication protocol with said requester through said control channel and discarding said request if said requester cannot be authenticated or is not authorized to request VLAN service from said bridge. It is disclosed by Gage et al of receiving said request frame initiating an authentication protocol with said requester through said control channel and discarding said request if said requester cannot be authenticated or is not authorized to request VLAN service from said bridge (col. 2, lines 17-44). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply authentication of parties in order to determine if they are authorized to gain access. The teachings of Gage et al recites motivation for the use of authentication by disclosing that it can keep track of which members belong to a VLAN and to avoid unauthorized parties connecting to a VLAN (col. 2, lines 7-10 & 20-26). It is obvious that the teachings of Yuasa et al would have been improved by incorporating the teachings of Gage et al as a means of ensuring that authentic parties are authorized to access a VLAN.

As per claim 25, it is taught by Yuasa et al of a system for segregating traffic amongst a plurality of stations that are associated with an access point, a method for

linking a new virtual local area network (VLAN) to one or more existing VLANs served by physical ports of a bridge, comprising the steps of sending a join-VLAN request over a control channel, adding a logical port that serves a source VLAN to a member set of every virtual LAN ID (VID) in a set of VIDs for VLANs served by a set of physical ports which comprise destination VLANs, and adding every physical port in said set of physical ports to a member set of said source VLAN; and forming an untagged set of said source VLAN by taking a union of all untagged sets for VIDs in said set of VIDs for VLANs served by a set of physical ports which comprise destination VLANs, wherein if a request frame contains a null VID in its tag header, or it is untagged, then a logical port of said bridge is added to an untagged set of every VID in set of VIDs for VLANs served by a set of physical ports which comprise destination VLANs (col. 7, lines 28-41; col. 9, lines 15-25 & 33-53; and col. 10, lines 48-67). The teachings of Yuasa et al are silent in disclosing of authenticating said request wherein, if authentication fails, said request is discarded. Gage et al discloses of authenticating said request wherein, if authentication fails, said request is discarded (col. 2, lines 17-44). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply authentication of parties in order to determine if they are authorized to gain access. The teachings of Gage et al recites motivation for the use of authentication by disclosing that it can keep track of which members belong to a VLAN and to avoid unauthorized parties connecting to a VLAN (col. 2, lines 7-10 & 20-26). It is obvious that the teachings of Yuasa et al would have been improved by incorporating

the teachings of Gage et al as a means of ensuring that authentic parties are authorized to access a VLAN.

As per claim 26, Yuasa et al teaches of 26. In a system for segregating traffic amongst a plurality of stations that are associated with an access point, a method for joining a personal virtual local area network (VLAN) served by a logical port, comprising the steps of if source and destination VLANs have a same creator, and said creator issued a join-VLAN request, then said request is discarded, if said source and destination VLANs are identical and said creator did not issue said request (col. 9, lines 15-25 & 33-45; col. 10, lines 48-67). Yuasa et al fails to disclose of a creator authenticates said requester for membership into said personal VLAN, and in all other cases, a bridge first authenticates said request to make sure that said requester is the creator of said source VLAN, wherein if authentication succeeds, then said creator authenticates said requester for membership into said destination VLAN; and wherein said requester authenticated said creator to make sure that said creator is the creator of said destination VLAN. It is disclosed by Gage et al of creator authenticates said requester for membership into said personal VLAN, and in all other cases, a bridge first authenticates said request to make sure that said requester is the creator of said source VLAN, wherein if authentication succeeds, then said creator authenticates said requester for membership into said destination VLAN; and wherein said requester authenticated said creator to make sure that said creator is the creator of said destination VLAN (col. 2, lines 17-44). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply

authentication of parties in order to determine if they are authorized to gain access. The teachings of Gage et al recites motivation for the use of authentication by disclosing that it can keep track of which members belong to a VLAN and to avoid unauthorized parties connecting to a VLAN (col. 2, lines 7-10 & 20-26). It is obvious that the teachings of Yuasa et al would have been improved by incorporating the teachings of Gage et al as a means of ensuring that authentic parties are authorized to access a VLAN.

As per claim 27, Yuasa et al teaches of a system for segregating traffic amongst a plurality of stations that are associated with an access point, a method for joining a personal virtual local area network (VLAN) served by a logical port, comprising the steps of providing a personal VLAN bridge having a control channel a requester by a creator (col. 9, lines 15-25 & 33-45; col. 10, lines 48-67). The teachings of Yuasa et al are silent in disclosing of authenticating a request, authentication of a requester by a creator, the personal VLAN bridge using said control channel to relay authentication protocol messages between said creator and said requester, and if said creator can authenticate said requester, then said creator sharing a security association it holds with said personal VLAN bridge with said requester as well. Gage et al discloses of authenticating a request, authentication of a requester by a creator, the personal VLAN bridge using said control channel to relay authentication protocol messages between said creator and said requester, and if said creator can authenticate said requester, then said creator sharing a security association it holds with said personal VLAN bridge with said requester as well (col. 2, lines 17-44). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply

authentication of parties in order to determine if they are authorized to gain access. The teachings of Gage et al recites motivation for the use of authentication by disclosing that it can keep track of which members belong to a VLAN and to avoid unauthorized parties connecting to a VLAN (col. 2, lines 7-10 & 20-26). It is obvious that the teachings of Yuasa et al would have been improved by incorporating the teachings of Gage et al as a means of ensuring that authentic parties are authorized to access a VLAN.

As per claim 28, Yuasa et al discloses of providing ingress filtering at logical ports (col. 7, lines 14-20).

As per claim 29, Yuasa et al teaches of security association contains at least two keys, one key for encryption and another key, wherein said security association is associated with a VLAN, wherein said authentication code is used to limit traffic at a logical port to members of an entire VLAN, wherein encryption is used to keep traffic private except to members, wherein only stations having said security association belong to said VLAN, and wherein all stations having said security association belong to the same broadcast domain (col. 45, lines 13-17). Gage et al is relied upon for disclosing of the use of authentication, please refer above as to the motivational benefits of the teachings of Gage et al as applied to Yuasa et al.

As per claim 30, Yuasa et al discloses that a physical port may serve more than one VLAN by having multiple logical ports associated with it (col. 79, lines 4-20).

As per claim 32, it is taught by Yuasa et al of a transmission port for a frame that belongs to a VLAN is not a member set of the VLAN, then the frame is discarded (col. 7, lines 14-20).

As per claim 35, it is disclosed by Yuasa et al of wherein said personal VLAN bridge extends a standard VLAN bridge in at least any of the following ways, a VLAN discovery in which a personal VLAN bridge provides a protocol for VLAN discovery, VLAN extension in which a personal VLAN allows a station to create a new port that serves a new VLAN, logical ports in which a personal VLAN bridge maintains more than one logical port per physical port, and bridges between ports of any kind; and cryptographic VLAN separation in which in a personal VLAN, a logical port serves at most one VLAN but, because there may be more than one logical port per physical port, more than one VLAN may exist on a physical port (col. 9, lines 3-15; col. 45, lines 13-17; and col. 79, lines 4-20). The teachings of Yuasa et al are silent in disclosing of joining an existing VLAN via an authentication protocol. Gage et al teaches of means for allowing a station to join an existing VLAN via an authentication protocol wherein the authentication code uniquely identifies a VLAN to which traffic belongs (col. 2, lines 17-44). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply authentication of parties in order to determine if they are authorized to gain access. The teachings of Gage et al recites motivation for the use of authentication by disclosing that it can keep track of which members belong to a VLAN and to avoid unauthorized parties connecting to a VLAN (col. 2, lines 7-10 & 20-26). It is obvious that the teachings of Yuasa et al would have been improved by incorporating the teachings of Gage et al as a means of ensuring that authentic parties are authorized to access a VLAN.

As per claim 36, Yuasa et al teaches that traffic within one VLAN is separated from another VLAN on a same physical port by cryptography (col. 45, lines 13-17 and col. 79, lines 4-20).

As per claim 37, Yuasa et al discloses that encryption keeps traffic private except to members of said VLAN (col. 45, lines 13-17). Gage et al is relied upon for disclosing of an authentication code uniquely identifies a VLAN to which said traffic belongs, please refer above as to the motivational benefits of the teachings of Gage et al as applied to Yuasa et al.

Allowable Subject Matter

6. Claim 31 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131

CR

September 25, 2005